Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("---") or ("[[ ]]") double brackets, as is applicable:

1. (Currently amended) A method for securely transmitting data between a computer and a printer, comprising:

converting a file for printing into a printer description language format;

encrypting said file in said printer description language format;

providing said file with an identifier ~~for the printer~~ in a header of said file that provides an indication of an algorithm that was used to encrypt said file; and

transmitting said file to the printer.

2. (Original) The method of claim 1, further comprising decrypting said file by the printer.

3. (Currently amended) The method of claim 1, wherein said converting comprises converting said file into at least one of a postscript format, a ~~.pcl~~ PCL format, a ~~.pdf~~ PDF format, and an ~~.xml~~ XML format.

4. (Currently amended) The method of claim 1, further comprising: receiving said file by the printer, the printer recognizing said identifier, validating said identifier, and selecting an appropriate decryption algorithm that is associated with the computer.

5. (Currently amended) The method of claim **[[4]]** 1, wherein said providing includes providing said header of said file with a flag recognizable solely by the printer for ~~indicating~~ identifying an encryption algorithm ~~for use~~ used in said encrypting.

6. (Canceled)

7. (Currently amended) The method of claim 5, further comprising ~~at least one of~~ recognizing said flag~~, validating said flag,~~ with the printer and selecting an appropriate decryption algorithm.

8. (Currently amended) The method of claim 7, ~~wherein said~~ further comprising validating said flag on the printer by ~~includes~~ entering a decryption key into the printer that corresponds to said flag.

9. (Canceled)

10. (Currently amended) The method of claim ~~2~~ 7, wherein ~~said decrypting comprises~~ selecting an appropriate decryption algorithm comprises selecting an appropriate decryption algorithm from a plurality of decryption algorithms available to the printer ~~based upon at least one of an identifier for the computer and a flag provided with said file~~.

11. (Currently amended) A method for securely transmitting data between a first device and a second device in a computer network, comprising:

encrypting a file ~~for transmitting~~ to be transmitted by the first device;

providing a header of said file with an identifier ~~for~~ that provides an indication of an algorithm that was used to encrypt said file; and

transmitting said file from the first device to the second device.

12. (Original) The method of claim 11, further comprising:

decrypting said file by the second device.

13. (Currently amended) The method of claim 12, ~~further comprising:~~ wherein encrypting comprises encrypting said file by employing one of a plurality of encryption programs available to the first device~~; providing said file with an identifier for the first device;~~ and further comprising performing on the second device prior to decrypting at least one of recognizing said identifier ~~for the first device~~, validating said identifier ~~for the first device~~, and selecting an appropriate decryption algorithm from a plurality of decryption algorithms.

14. (Currently amended) The method of claim 13, wherein said providing ~~said identifier for said file~~ includes providing a flag ~~for~~ in said header of said file, said flag recognizable only by the second device and ~~indicating an encryption algorithm~~ identifying which of said plurality of encryption programs was used to encrypt said file.

15. (Canceled)

16. (Currently amended) The method of claim ~~15~~ 14, further comprising performing with the second device at least one of recognizing said flag, validating said flag using a decryption key corresponding to said flag of the second device, and selecting an appropriate decryption algorithm from said plurality of decryption algorithms.

17. (Currently amended) A system for securely transmitting a file in a computer network, comprising:

a first device including at least one processor for providing an encrypted file with an identifier ~~for transmitting on said computer network~~ that provides an indication as to an encryption algorithm that was used to encrypt the file; and

a second device including at least one processor for decrypting and outputting the file.

18. (Currently amended) The system of claim 17, wherein ~~said at least one processor of~~ said first device includes at least one encryption algorithm.

19. (Currently amended) The system of claim 18, wherein said at least one processor of said first device ~~further includes a source for identifiers and flags recognizable solely by said second device for providing~~ is configured to provide the file header with ~~at least one of an identifier and~~ a flag ~~for indicating~~ that identifies an encryption algorithm ~~for encrypting~~ that was used to encrypt the file.

20. (Currently amended) The system of claim 19, wherein said second device further includes an input element for entry of a decryption key ~~separately from receipt of the file, said decryption key~~ for recognition by said at least one processor of said second device and for corresponding to at least one decryption algorithm available to said at least one processor of said second device and ~~a~~ said flag accompanying the file.

21. (Currently amended) The system of claim 17, wherein said first device comprises a computer and said second device comprises a printer, said first device having apparatus for converting the file into ~~an output format including~~ a printer description language format.

22. (Currently amended) The system of claim 17, wherein said first device includes at least one encryption algorithm ~~for corresponding~~ that corresponds to a decryption algorithm available to said second device ~~remotely in time from transmission of the file across the computer network~~.

23. (Currently amended) A printer, comprising:

at least one processor ~~for receiving~~ configured to receive an encrypted file for printing ~~from a computer~~ and ~~for receiving at least~~ configured to read an identifier ~~for said printer accompanying~~ provided in a header of said encrypted file, the identifier providing an indication of an encryption algorithm that was used to encrypt said file, said at least one processor ~~for executing~~ being configured to execute a decryption algorithm to decrypt said encrypted file ~~after receipt of said identifier~~; and

at least one printing element for printing ~~at least files decrypted by~~ said file ~~at least one processor~~.

24. (Original) The printer of claim 23, further comprising a memory connected to said at least one processor for storage of said decryption algorithm.

25. (Original) The printer of claim 23, further comprising:

at least one decryption algorithm associated with said at least one processor.

26. (Currently amended) The printer of claim 23, wherein said ~~at least one processor recognizes at least one of an~~ identifier ~~associated with a particular~~ identifies at least one of the source of said encrypted file and a ~~flag recognizable only by the printer and indicative of~~ an encryption algorithm ~~for encrypting~~ that was used to encrypt said encrypted file.

27. (Currently amended) The printer of claim 26, wherein said at least one processor selects a decryption algorithm for decrypting said encrypted file from a plurality of available decryption algorithms based upon ~~recognizing said at least one of~~ said identifier ~~and said flag~~.

28. (Currently amended) The printer of claim 26, further comprising an input element configured for receiving decryption key, said decryption key corresponding to said ~~flag for facilitating recognition thereof~~ identifier.

29. (Original) The printer of claim 28, wherein said decryption key facilitates activation of a decryption algorithm.